

Hal S. Shaftel (HS-0627)  
Daniel P. Goldberger (DG-2440)  
PROSKAUER ROSE LLP  
1585 Broadway  
New York, New York 10036-8299  
Telephone 212.969.3000

*Attorneys for Plaintiff Passlogix, Inc.*

UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF NEW YORK

-----	X	
PASSLOGIX, INC.,	:	
	:	
Plaintiff,	:	
	:	
against	:	Case No. 08 CV 10986 (PKL/MHD)
	:	
2FA TECHNOLOGY, LLC, 2FA, INC.,	:	
GREGORY SALYARDS and SHAUN CUTTILL,	:	
	:	
Defendants.	:	
-----	X	

**PLAINTIFF PASSLOGIX'S POST-HEARING REPLY MEMORANDUM**

**TABLE OF CONTENTS**

	<b><u>Page</u></b>
TABLE OF AUTHORITIES .....	ii
I. SALYARDS HAS NO ANSWER TO DISPOSITIVE COMPUTER RECORDS .....	2
A. The Computer Records Are Definitive .....	2
B. IP Spoofing Is Not Possible Here .....	4
II. SALYARDS AFFIRMATIVELY USED THE SEPTEMBER 3 EMAIL .....	6
III. NO CREDIBLE EXCULPATORY EVIDENCE EXISTS .....	7
A. No Basis For Finger-Pointing At Robinson For September 3 Email .....	7
B. Salyards Misplaces Reliance On Collier For The April 13 Email.....	9
C. Salyards' Friendly Restaurant Witnesses Do Not Support His Testimony .....	11
D. The Attachments To The September 3 Email.....	11
IV. SALYARDS' SPOILIATION OF CORE INFORMATION.....	12
V. ABSOLUTELY NO BASIS EXISTS FOR SANCTIONING PASSLOGIX .....	14
CONCLUSION.....	15

# **TABLE OF AUTHORITIES**

	<b><u>Page</u></b>
<u>Abdul-Matiyn v. Coughlin,</u> 1996 WL 1089984 (S.D.N.Y. Nov. 8, 1996).....	4
<u>Bank of China v. NBM LLC,</u> 359 F.3d 171 (2d Cir. 2004).....	3
<u>Bourne Co. v. MPL Commc'ns, Inc.,</u> 751 F. Supp. 55 (S.D.N.Y. 1990) .....	15
<u>D'Amico v. City of New York,</u> 132 F.3d 145 (2d Cir 1998).....	4
<u>In re Enron Creditors Recovery Corp.,</u> 376 B.R. 442 (Bankr. S.D.N.Y. 2007).....	4
<u>Menashe v. V Secret Catalogue, Inc.,</u> 409 F. Supp. 2d 412 (S.D.N.Y. 2006).....	15
<u>Pension Comm. of the Univ. of Montreal Pension Plan, et al., v. Banc of America Sec.</u> <u>LLC, et al.,</u> --- F.R.D.--, 2010 WL 184312 (S.D.N.Y. Jan 15, 2010).....	12
<u>Sauer v. Xerox Corp.,</u> 5 Fed. Appx. 52 (2d Cir. 2001).....	15
<u>SEC v. 800America.com, Inc.,</u> 2006 WL 3422670 (S.D.N.Y. Nov. 28, 2006).....	4

When the falsehoods and rhetoric of Salyards' opposition brief ["Opp."] are unpacked, the genuine facts remain clear: extensive, unbiased computer records specifically tie Salyards to the transmittal of the September 3 Email (and the April 13 Email); he immediately interjected the September 3 Email into the case; and – despite extensive discovery – no credible exculpatory evidence of any other source exists.

Salyards repeatedly makes conclusory statements unsupported – indeed, refuted – by the actual record.<sup>1</sup> As a further distraction, Salyards devotes much attention to groundless assertions – irrelevant to the issue of the emails – about both discovery disputes and underlying claims in the case.<sup>2</sup> Ignoring the facts, Salyards accuses Passlogix of using the email issue for delay [Opp. at 2, 3]; not only has Passlogix never requested any delay, but – since November – it is Salyards/2FA who over Passlogix's objection twice (to no avail) sought to adjourn the end of discovery. [11/18/09 Tr. 4:6-9; 12/21 Order.] Although Salyards tries to kick up a lot of dirt, none of it obscures his clear culpability for the September 3 Email and his continuing deceit.

---

<sup>1</sup> Without identifying each unsupported or miscited assertion, examples include: Opp. at 6 (misleadingly truncates the Magistrate Judge's directive); Id. at 8 (misleadingly truncates Boroditsky testimony to omit fact that Passlogix objected to requested discovery); Id. at 15 (states that "Obuchowski testified that IP spoofing can be done in different ways," yet the citation [Tr. 145:15] has nothing do with this mischaracterization); Id. at 16-17 (states that Obuchowski did not know how AT&T recorded time zones, yet cites to [Tr. 22:3-12] an unrelated exchange between the Court and Passlogix's counsel during Boroditsky's testimony); Id. at 21 (states that Google China and Google Russia are the appropriate search engines to find "hacker programs," yet cites to [Tr. 364:3-365:1] an unrelated exchange).

<sup>2</sup> See, e.g., Opp. at 5 (states Passlogix did not produce unredacted attachments, yet the request for the information and other discovery expansions were denied by the Magistrate Judge); Id. at 6 (same); Id. at 26 (disputes the propriety of Passlogix's subpoena approved by the Magistrate Judge); Id. at 1 (argues merits of 2FA's preliminary injunction without addressing dispositive contrary proof); Id. at 1 ("Passlogix's complaint is meritless," yet no dismissal motion made).

I.

**SALYARDS HAS NO ANSWER TO DISPOSITIVE COMPUTER RECORDS**

A. **The Computer Records Are Definitive:** Objective computer records show the originating IP address for every action associated with both the September 3 and April 13 Email accounts. The only IP addresses captured – out of 86 separate actions recorded by the Hush website through which the emails were transmitted – are directly linked to Salyards: his home, his office, and the Mark Hopkins Hotel in San Francisco when he was a guest. [App. B.] This clear evidence singularly – and conclusively – identifies Salyards.

With nothing to say, Salyards largely ignores the record. He nowhere addresses the fact that the April 13 Hush Log captures his IP addresses as he moves from his office to his home in Austin; from Austin to the Mark Hopkins Hotel; and from San Francisco back to Austin. [App. B.] Nor does he ever address how, within a 23-hour period, the IP address captured by Hush changes from his office to his home and then back to his office. [App. B.] This shifting is crucial because it occurred while Salyards indisputably did not communicate by email with Collier (who claims he “spoofed” the April 13 Email), rendering specious any argument that Collier could have copied the shifting IP addresses to spoof in this timeframe.

For the period of Salyards’ stay at the Mark Hopkins, the internet records further show: (1) that the Hush account was accessed from the hotel on April 20 and 23; (2) that Salyards was a guest at the hotel on both days; (3) that both log-ins occurred while a computer was actively connected to the internet from a room for which he paid; and (4) that except for Cuttill, no other person associated with these matters has ever been identified as being at the hotel in this period.

By exaggerating an unremarkable absence of technical details in the Mark Hopkins customer bills, Salyards argues that the information “actually proves Mr. Salyards did not have anything to do with the April email.” [Opp. at 18.] But Salyards distorts the fact that the Hush

log identifies an IP address ending in “.2” while the Mark Hopkins bill identifies another IP address, with the same first eight digits, but ending in “.12.” This is a red herring: (1) it is undisputed that the “.2” IP address is registered to the Mark Hopkins [Tr. 158:15-159:2]; (2) in fact, Salyards’ bill shows a room without a specific assigned IP address for the relevant times; the hotel only assigned the specific “.12” IP address when a higher level of service was purchased, while Salyards had a room with lower service at the two times the Hush account was accessed [Tr. 186:1-13; 191:23-192:20; 195:24-196:8; 240:21-241:16.]; and (3) even when the “.12” IP address was internally assigned for billing records, outbound internet traffic is also routed through other hotel IP addresses, which include the “.2” IP address shown on the Hush log. [Tr. 191:8-22; 194:14-19; 613:3-614:20; 617:21-618:8.]

Furthermore, Salyards’ claim (if accepted) that he never used the “.2” IP address reflected on the Hush log actually negates his spoofing defense. If this were true, then no “spoofers” could have done so either – and it therefore would not appear on the Hush log. In any event, Salyards’ self-serving claim that he sent Collier an email from the hotel on April 19 with the “.12” address (not “.2”) cannot be credited because no copy exists, Salyards says he destroyed it, and Collier testified he received no such email.

As further explained by Obuchowski, the Mark Hopkins records show the “start” of an internet connection from Salyards’ room within a minute of a connection to Hush. [162:13-15] That timing is far too exact to be coincidental. To distract from this incriminating timing, Salyards asserts that the “start” for internet connectivity corresponds to when Salyards’ computer was powered on, which he claims is before connection to the internet.<sup>3</sup> [Opp. at 18.] Even

---

<sup>3</sup> The only support for this is the lay testimony of Cuttill, who has no basis, let alone qualifications, to opine on such matters. See e.g., Bank of China v. NBM LLC, 359 F.3d 171, 181, 182 (2d Cir. 2004) (not appropriate lay testimony where a witness seeks to proffer

though Salyards states “Obuchowski actually confirms” this [Id.], his testimony is squarely to the contrary: “start” time “signifies a connection to the hotel network . . . to gain access to the Internet.” [Tr. 611:6-8.] Obuchowski identifies “start” with an actual internet connection based on “years in law enforcement conducting hundreds of investigations involving computer crime” where he “examined dozens of hotel records, and these entries in the hotel records of ‘start,’ ‘end’ are pretty consistent.” [Tr. 611:15-19.]

**B. IP Spoofing Is Not Possible Here:** In the face of unassailable computer data and other evidence, Salyards resorts to a far-fetched theory of IP address spoofing. But that “wholly fanciful” challenge is inadequate to undercut the documentary record. D’Amico v. City of New York, 132 F.3d 145, 149 (2d Cir 1998) (party “may not rely on mere conclusory allegations nor speculation” in lieu of “hard evidence”); SEC v. 800America.com, Inc., 2006 WL 3422670, at \*7 n.5 (S.D.N.Y. Nov. 28, 2006) (rejecting assertion that someone forged documents where “the record does not support [] claim”); Abdul-Matiyn v. Coughlin, 1996 WL 1089984, at \*17 (S.D.N.Y. Nov. 8, 1996); (“mere accusations of . . . false documents, without more,” is insufficient to overcome presumption of reliability); see also In re Enron Creditors Recovery Corp., 376 B.R. 442, 455 (Bankr. S.D.N.Y. 2007) (“data from the entity’s computer system . . . bear sufficient indicia of trustworthiness”).

Obuchowski’s expert conclusions are unrebutted that (1) there is no software on the market that can spoof public IP addresses assigned by an ISP, such as the IP addresses assigned by Time Warner and recorded by Hush [Tr. 164:6-19; 242:13-16; 623:17-624:2]; (2) that IP spoofing is not technologically feasible here where a two-way connection existed between Hush and a user (because Hush would have sent communications back to Salyards, not the spoofer).

---

testimony that reflects specialized knowledge; accordingly, such testimony must satisfy the reliability requirements concerning expert witnesses set forth in Rule 702).

[Tr. 615:8-16]; and (3) that internet records show no spoofing took place.<sup>4</sup> [PX 36 at ¶¶ 3-15; Tr. 168:21-169:16; 170:15-18; 616:20-617:4.] Even though Salyards and Cuttill claim to have IP “spoofed” in the past [Tr. 391:2-4; 565:9-566:4], it related to authorized testing, which (very different from here) did not involve two-way communications with a website, nor misuse an unknowing person’s public IP address assigned by a service provider like Time Warner.

Rather than try to rebut the technical aspects of Obuchowski’s conclusions, Salyards simply proclaims that Obuchowski “lacks credibility”. [Opp. at 15.] But Salyards cannot be serious: in addition to being qualified (without objection) as an expert by this Court, Obuchowski also has been qualified in federal court elsewhere on IP spoofing; he spent 12 years in law enforcement, where, as a member of a computer crime task force, he conducted hundreds of computer crime investigations; and he teaches computer forensics at both colleges and police academies in Massachusetts. [PX 36 at ¶ 1, Ex. 1; Tr. 145:11-146:18.]

Ignoring the technological limitations of IP spoofing, Salyards also argues that Obuchowski did not understand Collier’s testimony: although Collier clearly testified that he used the “MacIP Change” software, Salyards states “Collier appears to have been referring to a generic software program, not a specific one.” [Opp. at 20.] The record, however, speaks for itself: (1) when Collier identified Mac IP Change, he stated it “is one that I’ve used many times before. That’s the one I used.” [Collier Tr. 86:23-25] (emphasis added.); (2) there were ten separate log-ins to the April 13 Email account – meaning (had he been the source) he obviously would have known what program he used; (3) even if Collier had been speaking about “a generic software program” (he clearly was not), it is irrelevant because there is no software on

---

<sup>4</sup> As Obuchowski testified, spoofing would leave indicia in the internet records, such as inconsistencies in the header data [PX 36 at ¶ 15], but no such indicia are present here. [PX 36 at ¶¶ 14-15; Tr. 168:21-169:16; 616:20-617:4.]

the market that can be used to spoof an IP address assigned by an internet service provider as here. [Tr. 242:12-16; 623:17-624:2.]

Even if “spoofing” were technologically possible (which it is not), Salyards’ spoofing defense is nonsensical and thus cannot be credited: some unknown person, for some unknown reason, wrote the September 3 Email claiming to be a Passlogix employee, but then (using phantom technology), made it appear as if it had been sent by Salyards. Since the author claimed to work at Passlogix, then why would he – in the off chance that the internet service provider were subpoenaed – spoof an IP address so that the data would reflect a non-Passlogix employee (i.e., Salyards)? The fundamental facts and logic – which Salyards cannot combat – unequivocally demonstrate that Salyards was the source of the emails at issue.

## II. **SALYARDS AFFIRMATIVELY USED THE SEPTEMBER 3 EMAIL**

Recognizing the strength of the clear, objective computer records and other evidence, Salyards argues that – regardless of who sent the September 3 Email – “2FA has not submitted [it] to the Court” and by extension no fraud occurred. [Opp. at 5.] But Salyards’ characterization is utterly disingenuous: in fact, the (phony) email purports to reflect the views of a Passlogix employee concerning intellectual property matters at issue in the case, and was circulated in a manner (with 2FA copied) so as to ensure it became part of the record. On cue, Salyards and 2FA immediately exploited the email to manipulate the judicial process. Within 24 hours of the email, Salyards’ counsel wrote to Passlogix’s counsel that his clients take the email “very seriously” and demanded broad production of documents based on the email – including information about a development project that Passlogix previously (and successfully) had objected to producing. [PX 58.] Next, Salyards himself wrote to Passlogix about the email, using it expressly as leverage for his settlement proposal in advance of the scheduled settlement

conference before the Magistrate Judge, and specifically stating that “[o]ur attorney plans on raising the issue with the court this week.”<sup>5</sup> [PX 29.] His counsel then wrote the Magistrate Judge on September 14 “to bring to [the Court’s] attention an anonymous email received by 2FA,” and asserting the need for additional, expansive discovery on the basis of the email. [PX 30.] To further highlight the email, Salyards’ counsel’s letter describes it as a “developer stating . . . he believes there is a serious issue regarding Passlogix’s use of third parties intellectual property.” [PX 30.]

Because Salyards’ counsel characterized the email to the Court without including an actual copy (but stated he would do so if requested), Passlogix’s counsel submitted it for the Court’s review. Although Passlogix provided the email in response to Salyards/2FA’s assertions, it is undeniable that Salyards/2FA first raised it and described it to the Court, and used it for both settlement leverage in connection with a judicially supervised settlement conference, and as a means for arguing for additional, intrusive discovery from Passlogix. In these ways, Salyards’ use of the email was directed at interfering with the judicial process and clearly constitutes a serious fraud on the Court. [See cases cited in Passlogix Mem. at 28-30.]<sup>6</sup>

### III.

#### **NO CREDIBLE EXCULPATORY EVIDENCE EXISTS**

A. **No Basis For Finger-Pointing At Robinson For September 3 Email:** As he tries to identify some possible alternative source for the September 3 Email, Salyards asserts that “there is persuasive evidence that Joe Robinson sent this email.” [Opp. at 2, 4, 13.] However,

---

<sup>5</sup> Hypocritically, Salyards claims “settlement offers and negotiations are not evidence” [Opp. at 33, n.9]; yet, he himself mischaracterizes settlement discussions. [Id. at 2 n.3.]

<sup>6</sup> Although Salyards principally seeks to distinguish these cases by stating the September 3 Email was not “central to the truth-finding process” [Opp. at 28], that is a gross mischaracterization: the email purports to relate to the subject of the case; Salyards promptly exploited it; he also pressed Passlogix to spend substantial resources investigating it, thereby diverting litigation resources.

there is absolutely no competent, credible evidence linking Robinson to the email; indeed, the record is flatly to the contrary. Salyards relies solely on the (inadmissible) speculation of his friend Collier. But Collier admits he does not know who sent the email [Collier Tr. 65:16-17]; he had not even spoken to Robinson for three months before the email [Id. 77:17-78:12]; and he had no knowledge of misuse of any intellectual property at Passlogix. [Id. 97:2-16.] Contrary to Salyards' specious finger-pointing, a multitude of facts refute Robinson being the source:

The contents of the email do not fit Robinson, such as the reference to "a monthly paycheck", when Robinson received bi-weekly pay (exactly the type of mistake an imposter would make); the reference to "stop assisting", when Robinson had just resumed work after an excused medical leave; the reference to being treated like a "second-class citizen" by Marc Manza, when Robinson did not recently interact (or ever regularly interact) with Manza;<sup>7</sup> the reference to "additional information that I will share", when neither Robinson nor anyone else has provided anything additional [Tr. 468:8-469:5]; and other inconsistencies between the description of the author's background and Robinson's work experience. Indeed, Robinson himself expressed positive views about Passlogix to the internal investigation interviewers. [DX 12 at PL0096104.]

The text of the email also includes U.K./Canadian spellings for certain words, while Robinson in his own writings consistently uses the American spellings. [DX 16.] Usage of U.K. spellings is an easy means for an imposter to make it appear as if the author was one of Passlogix's Canadian-based developers, and Salyards knew of these employees. [438:25:439:12.] Even Salyards' own proffered linguist does not believe Robinson wrote the email. [Tr. 308:2-6.] Salyards even goes so far as to argue "if the email was dictated, it would have reflected

---

<sup>7</sup> However, it is telling that Salyards himself previously emailed virtually the same verbiage about being "treated . . . like second class citizens" to describe Passlogix management. [PX 9.]

Mr. Robinson's thoughts" but not his "style and writing practices." [Opp. at 24.] There is no indicia whatsoever, let alone evidence, that the email was dictated to some mystery third party – and such make-believe scenarios should be rejected out of hand.

In a last-ditch effort to finger Robinson, Salyards states that "Robinson was very concerned about being asked to use IdentiPHI code while working at Passlogix." [Opp. at 13-14.] However, this misstatement is plainly contradicted by Collier's testimony about Robinson:

So, the code that I was asking Mr. Robinson to take a look at was property of a customer. I just wanted to clarify it was not property of . . . IdentiPHI, nor Imprivata . . . it was not property of a previous employer. [Collier Tr. 79:7-18] (emphasis added.)

Likewise, Robinson explained to the internal investigators that Collier asked him to work on certain customer code, not prior employer or 2FA code – which he in fact never did do after obtaining guidance from his supervisor at Passlogix, and then described the incident as "not a big deal." [PX 35 at PL0095991.] Compelling evidence thus excludes Robinson as the email author.

**B. Salyards Misplaces Reliance On Collier For The April 13 Email:** To begin with, it is critical to emphasize that Collier's testimony has nothing to do with the key September 3 Email (it only relates to the April 13 Email, which – while it corroborates Salyards' pattern of conduct with anonymous Hush emails – is not the email pertinent to activities in the case). Insofar as the April 13 Email is concerned, Collier is clearly a biased witness, since he and Salyards engaged in extensive secret business dealings, and they are in regular social contact. Although Salyards blithely asserts that "Collier is a credible witness" [Opp. at 10], Collier's testimony is riddled with inaccuracies and inconsistencies left unaddressed by Salyards:

- As noted above, Collier's testimony about IP spoofing is not technologically feasible.

- Collier testified incorrectly about basic facts concerning the April 13 Email, including the date the account was set up, and the password he used to create the account.<sup>8</sup> [Passlogix Mem. at 21-22]
- Collier testified that he did not know Salyards was in San Francisco in April and did not email with him there. [Tr. 63:19-22; 126:16-127:4.] However, Salyards claims that Collier knew he was in San Francisco and that he sent Collier an email (allegedly discarded and not produced) from the hotel whose IP address Collier allegedly spoofed. [Opp. at 18.]
- Collier testified that Cuttill was the source of the information contained in the April 13 Email. [Collier Tr. 108:15-22.] Yet, 2FA denies that Cuttill was the source, even though much of the information in the email was not known by Collier, since he had only worked at Passlogix for twelve days when the email was sent. (The fact that Cuttill was the source further negates Salyards' claim the email somehow was harmful to 2FA; indeed, it specifically describes a person having "a lot of respect" for Salyards.)
- Collier's testimony was contradicted by the expert testimony from Passlogix's computer forensic expert, Douglas Brush, who found that at the time the April 13 Email was sent from 2FA's offices, Collier's other computer was being used by a user named "chrisc" with the full name of "Chris Collier" at a different location.<sup>9</sup> [486:16-20; 492:5-13.]

Salyards also misrepresents his relationship with Collier, claiming that "[i]t is disputed whether or not Passlogix knew Chris Collier was working with 2FA." [Opp. at 11, n. 9.] There is no dispute. Collier's supervisor, Bonnell, clearly testified: (1) he did not know Collier was working with 2FA [Tr. 106:6-107:6]; to the contrary, Collier told Bonnell that he wanted to "steer clear" of 2FA because he did not want to get "caught in the cross hairs of the lawsuit" [Tr. 106:11-16]; (2) that Collier's job responsibilities did not include working with 2FA [Tr. 106:6-7]; and (3) that working with 2FA was "inappropriate" and "unauthorized" [Tr. 108:14-18.]

Nor does Salyards ever address why he and Collier communicated ten times (including a twelve minute early morning call) within 16 hours of Passlogix's letter to the Court about the

---

<sup>8</sup> Salyards suggests that Collier's failure to identify the correct password is irrelevant because Obuchowski also could not remember the test password he used once to create a Hush account. [Opp. at 16.] But there is an important distinction: the author of the April 13 Email used the password ten separate times, and Collier claimed he recalled it. [Collier Tr. 85:8-18.]

<sup>9</sup> Salyards attacks Brush's qualifications (ignoring his 15 years of forensic experience), because Brush does not have a college degree [Opp. at 21] – though neither does Salyards, who offered testimony on technical computer issues. [Tr. 371:25-372:8; 388:19-23; 390:15-392:25.]

emails – all Salyards misleadingly states is that the logs show three calls [Opp. at 12 n. 1], but he omits the seven text messages. Based on compelling evidence, it is clear that Collier’s testimony – which is not even relevant for the September 3 Email – does not add up and any claim he surreptitiously spoofed his friend’s IP address is not tenable.

**C. Salyards’ Friendly Restaurant Witnesses Do Not Support His Testimony:**

Salyards’ erroneously states that “three of the witnesses placed Mr. Salyards at the restaurant at the crucial time” the September 3 Email was sent. [Opp. at 12.] To the contrary: (1) each witness admitted that their recollections were estimates at best [Passlogix Mem. at 13-14]; (2) one of the witnesses testified that Salyards arrived after the email was sent [Dismore Tr. 10:8-10:]; (3) only two (not three) remember him there at the “crucial” time; yet both remember him arriving at different times (and each consumed at least three pints of beer) [Passlogix Mem. at 14]; and (4) the restaurant witnesses could not even remember when they themselves arrived [Id. at 14.] In addition, Salyards claims he went back to the restaurant, and paid with his credit card, but none of the witnesses recalled him doing so and he never produced any confirmatory credit card receipt – as the Court specifically requested at the November 9 hearing. [Id. at 14.]

**D. The Attachments To The September 3 Email:** Salyards argues there is no proof that he was in possession of the attachments to the September 3 Email. [Opp. at 5.] However, it is uncontroverted that (1) his friend Collier had the very attachments on his laptop computer at the pertinent time [Tr. 484:5-9]; and (2) the two had approximately 150 written communications in eight months but Salyards destroyed each one. [Tr. 354:21-355:18.] The fact that Collier had the attachments shows that Salyards had easy access. In fact, Collier’s log of electronic Skype communications reveals Salyards asking about access to proprietary Passlogix data (i.e., AdminiTrack) during the course of the litigation. [PX 50 at PL00961801.] Salyards also

testified that he himself received from an “anonymous” source in June/July computer specifications similar to the September 3 Email attachments. [356:12-357:17.]

Given Salyards’ extensive, secret dealings with Collier – who had the attachments at the ready – and his destruction of pertinent written communications, the compelling inference is Salyards had easy access to the attachments. The destruction of records should preclude Salyards from arguing otherwise. As a defense to clear forensic computer evidence, Salyards has no basis to argue that he lacked access to the attachments; he clearly had access.

#### IV. **SALYARDS’ SPOILIATION OF CORE INFORMATION**

During the pendency of this case, Salyards admits he never implemented any document preservation policy. [Tr. 353:9-14; 449:23-450:1.] This alone warrants sanctions. See Pension Comm. of the Univ. of Montreal Pension Plan, et al., v. Banc of America Sec., LLC, et al., --- F.R.D. ---, 2010 WL 184312 at \*3 (S.D.N.Y. Jan. 15, 2010) (“the failure to issue a written litigation hold constitutes gross negligence”). He deleted approximately 150 email and other written communications with his key witness Collier. [Tr. 354:21-355:18.] He also destroyed a claimed anonymous email he received in June/July 2009 from the Hush website attaching computer specifications similar to the attachments to the September 3 Email [Tr. 356:1-359:1.] By discarding this basic information, Salyards made it far more difficult and less efficient to test his claims about the nature of his communications and relationship with Collier; to confirm the whereabouts of each of them at pertinent times; and – particularly if the June/July anonymous Hush email actually existed – to trace the source of the anonymous emails at issue.

In the face of his admitted repeated destruction of records, Salyards resorts to arguing he had no reason to maintain any of the information. But that clearly is not so. On its face, the information was relevant to the case: he is in active litigation with Passlogix and is

communicating about business matters with only one Passlogix employee – albeit, unbeknownst to anyone else at Passlogix.<sup>10</sup> [Tr. 106:6-16.] Nothing in logic or law justifies his destroying communications during the lawsuit with the one person with whom he was interacting on the side – who also happens to become his key witness. He communicated with Collier about product bugs and maintenance matters at issue in the case; indeed, he apparently communicated about the Passlogix AdminiTrack system that was the very subject of discovery disputes before the Magistrate Judge. [Tr. 460:9-462:10.] Furthermore, the claimed anonymous June/July email attaching Passlogix computer specifications – which Salyards spent upwards to an hour reading but never disclosed to Passlogix for over three months [Tr. 358:13-15] – involves intellectual property that 2FA itself contends relates to the lawsuit. [Opp at 5.]

Salyards' own conduct further belies any good faith in deleting these records. He claims he does not maintain routine emails from Collier, but retained other routine emails. [Tr. 354:21-355:18.] He claims he did not maintain his alleged email with Collier from San Francisco when he was at the Mark Hopkins hotel, yet kept other emails from that period. He pressed for expansive discovery based on his review of the computer specifications attached to the September 3 Email, but would have the Court believe he deleted similar specifications in June/July without saying anything to anyone (except Cuttill). [Tr. 357:23-358:5.]

Thus, it is clear that Salyards destroyed core information that should have been preserved and thereby prejudiced Passlogix's ability to develop the factual record further and increased Passlogix's costs in investigating these email-related matters. Under these circumstances, Salyards should be precluded from making arguments implicating the destroyed information –

---

<sup>10</sup> Collier only communicated with Salyards' through his personal email account; not his Passlogix account. Thus, Salyards' contention that "Passlogix has [Collier's] emails" [Opp. at 30] is disingenuous.

including his entirely unsupported claim that he emailed Collier from the Mark Hopkins, and that is how Collier could have known the IP address of the hotel at which he was staying. In addition, his misconduct provides a further basis for the imposition of costs to compensate Passlogix for its activities in investigating these email-related matters. [See cases cited in Passlogix Mem. at 34.]

## V.

### **ABSOLUTELY NO BASIS EXISTS FOR SANCTIONING PASSLOGIX**

In an effort to obfuscate his own wrongdoing, Salyards argues – contrary to the facts and law – for the imposition of sanctions on Passlogix. Far from any impropriety on its part, Passlogix has acted responsibly and in good faith in all respects when addressing these matters: Passlogix first conducted through outside counsel a thorough, costly investigation before examining any external source for the email; Passlogix then undertook a forensic analysis of objective, non-party computer records; it then (in stark contrast to Salyards) was forthcoming in providing pertinent disclosures, including waiving the attorney-client privilege with respect to internal investigation matters, and making eight employees available for depositions and producing additional personnel and other records in response to Salyards’ requests. As the Magistrate Judge previously observed: “We see no basis for inferring that [Passlogix] has not met its discovery obligations . . . and defendants offer none.” [11/24/09 Order at 2.] Salyards’ irresponsible rhetoric about Passlogix somehow “fabricating” [Opp. at 4, 5, 8, 34] information is entirely without support.<sup>11</sup>

Even were this Court to find that Passlogix has not met its burden of proof in demonstrating Salyards’ culpability (which Passlogix respectfully believes it has done), there

---

<sup>11</sup> Contrary to Salyards’ similar rhetoric regarding the attachments, Passlogix never “concealed attachments” [Opp. at 5]; rather Passlogix produced them in redacted form, faithful to the Magistrate Judge’s instructions permitting it to do so.

still is no basis for any sanctions on Passlogix. Unlike Passlogix's request for costs based on proof of Salyards' deceitful, perjurious conducts, there is – on any view of the facts – no bases recognized by law for sanctioning Passlogix.<sup>12</sup> Sauer v. Xerox Corp., 5 Fed. Appx. 52, 57 (2d Cir. 2001) (“[A]lthough [suit was] ultimately adjudged to be without merit,” no recovery for attorneys' fees because suit could not “be fairly characterized as ‘entirely without color’” (internal citation omitted); Menashe v. V Secret Catalogue, Inc., 409 F. Supp. 2d 412, 427 (S.D.N.Y. 2006) (rejecting claim for attorneys' fees where “there [was] nothing in [the] record to suggest that” unsuccessful claim was brought “vexatious[ly] or wanton[ly]”); Bourne Co. v. MPL Commc'ns, Inc., 751 F. Supp. 55, 57 (S.D.N.Y. 1990) (“attorneys' fees are incidents of litigation and a prevailing party may not collect them from the losing party unless such an award is authorized by agreement between the parties, statute or court rule”).

### CONCLUSION

Accordingly, Passlogix respectfully requests that this Court dismiss Salyards/2FA's pleading and impose costs on Salyards for Passlogix's investigation of the September 3 Email.

Dated: February 15, 2010

PROSKAUER ROSE LLP

By: Hal S. Shaftel  
 Hal. S. Shaftel (NS-0627)  
 Daniel P. Goldberger (DG-2440)

Proskauer Rose LLP  
 1585 Broadway  
 New York, NY 10036  
 Tel. (212) 969-3000  
 Fax (212) 969-2900

*Attorneys for Plaintiff Passlogix, Inc.*

---

<sup>12</sup> It is particularly hypocritical for Salyards to seek costs, when he just recently expanded the parties' disputes and increased costs by filing a new lawsuit in Texas involving the same email accusations at issue here. See 2/11/10 Ltr. from H. Shaftel to Hon. Peter K. Leisure.